Notes

Contact

For questions or to learn more about the DHS National Cyber Exercise and Planning Program (NCEPP), please contact: *CEP@hq.dhs.gov* | (703) 235-5641

Homeland Security

Mile High DICE Tabletop Exercise

November 10, 2016

Exercise Purpose

- Mile High DICE provides a forum for interagency coordination and improvement of continuity and response plans.
- The 2016 theme is cybersecurity, which is the RISC (Regional Interagency Steering Committee) priority this year.
- DICE establishes a learning environment for participants to improve their understanding of a cyber incident and examine response/contingency plans to determine their ability to continue their mission essential functions.

Objectives

- Develop a common understanding of:
  - » Cybersecurity threats and vulnerabilities
  - » Cyber resources available from the government
- Identify cyber gaps or vulnerabilities that could disrupt delivery of mission essential functions.
- Discuss response and recovery of mission essential functions following a cyber event.
- Deliver sample tools that will assist in the development of a cyber annex in the organization's plan(s).

Exercise Facilitator

Jim Harris

- Department of Homeland Security - National Cybersecurity & Communications Integration Center (NCCIC) - National Cyber Exercise & Planning Program (NCEPP)
- Engineer/scientist for IBM in the mid-nineties
- Joined FBI after 9/11, served in Cyber Division, final assignment as Assistant Section Chief of Counterterrorism Internet Operations.
- Consultant for public and private sector companies for planning and preparing for cyber incidents since 2013.

GROUND TRUTH

Current Exercise Date

November 10, 2016

State of the World

- With the advent of the digital age and our reliance on electronics ranging from mobile devices to Bluetooth-enabled vehicles, we have gained several benefits such as efficiency and convenience.
- Taking advantage of weak cybersecurity policies and measures, malicious actors navigate these weaknesses with relative ease, capturing valuable information. The attacks can be in the form of brute force attacks, distributed denial of service (DDoS) attacks, phishing, Trojans, and others.
- Ransomware has provided a lucrative means to attack all types of sectors to include medical and education sectors. These particular attacks have increased throughout 2016.

Scenario Vignette 1: Ransomware Attack

Discussion Questions

- **What actions do you initially take?**
- **Describe your current cybersecurity-related policies. What protocols/policies are in place for downloading files?**
- **Does your organization provide basic cybersecurity awareness training to all employees (including managers and senior executives)? How often is training provided?**
- **Is training provided to new employees before they access your information systems?**
- **What other resources are available to assist your organization in a cyber incident?**
- **Do you pay the ransom? Why or why not?**

Digging for Gold – Day 1

- Law enforcement, IT officials, and other security staff review their respective daily/weekly intelligence and information products from various government and private sector sources, noting the rise in ransomware occurrences.
- The HR department in an organization receives an email from a prospective employee requesting advice on applying for a job. The email contains a resume in an attached PDF. The prospective employee provides information about the attachment and a cover letter describing why he is the perfect candidate for a particular job opening.
- Several recruiters (or hiring managers) open the attachment to look at the application and some reply offering advice to the prospective employee.

Digging for Gold – Day 3

- A few days later, employees are unable to log into their systems and a screen displaying a message, similar to the one below, appears on their screens. The message states all files are encrypted and 100 Bitcoins are required to be paid to unencrypt the files.

Scenario Vignette 4: Insider Threat

Discussion Questions

- **What are your highest-priority actions when a cyber attack occurs?**
- **How are actions coordinated across departments/ agencies?**
- **Who (e.g. agency, organization, etc.) is responsible for the big picture (i.e. collating information across multiple reports and sources)?**
- **When would you engage with local law enforcement?**
- **Describe your cyber threat information sharing mechanisms, products, and other considerations internal and external to your organization?**
- **Are processes in place for evidence retention, to aid in potential prosecution?**

The Usual Suspects

- Organizations, concerned with hackers attempting to get into their networks, are beginning to look more closely at insider threats, both malicious and unintentional, which can have serious repercussions.
- The biggest impact of an insider breach experienced by some organizations has been damage to brand or reputation and, to a lesser degree, intellectual property loss or financial loss.
- Insider threats continue to be a serious problem, mitigation programs can help organizations strengthen their position against internal threats by providing early detection of threats and a quick response.
- Insider threats with malicious intent have different motivations, such as money, pride/ego, ideology, or other reasons.
- Tools that these malicious actors might use could include downloadable malicious files, corrupted USBs/files/ websites, or a device that acts as a password sniffer similar to the below example:

- D-day: Employees arrive at their workstations and begin to work on their respective tasks. Nearly all employees bring their personal phones to work and charge them while at work. Phone chargers are everywhere. A disgruntled employee plugs his phone charger into an outlet near several employees who are working on a sensitive project.
- D+1: Some employees notice their files are missing and not organized. Help desk personnel are able to locate some files but not all.
- D+2: Several employees receive notifications from their banks about suspicious account activity. Additionally, the organization receives an alert that details of a sensitive project have been discovered on the dark web and the details of the project is for sale.
- D+5: Employees continue to report missing or corrupted files, leading IT personnel to investigate the issue.
- D+7: Upon further investigation, IT personnel discover the employees were logged on in nearly sequential times throughout the past five days. Log activity shows several amounts of data had been transferred to an outside IP address.
- D+8: The disgruntled employee quits work.
- D+8: Law enforcement is contacted and subsequently arrests the wayward coworker, confiscating his computer and other electronic devices.